UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,297	07/22/2003	James W. O'Toole JR.	1004-120	7810

47654 7590 01/15/2008		

BAINWOOD HUANG & ASSOCIATES LLC
2 CONNECTOR ROAD
WESTBOROUGH, MA 01581

EXAMINER
ALMEIDA, DEVIN E

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
01/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

		Application No.	Applicant(s)
Office Action Summary		10/624,297	O'TOOLE ET AL.
		Examiner	Art Unit	
		Devin Almeida	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _24 October 2007_.
2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _17,32,37,38 and 43-52_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) _17,32,37,38, and 43-52_ is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 10/24/2007.

Response to Arguments

Applicant's arguments that Chainer does not teach "implementing a recognition algorithm to identifying objects associated with the sensed images and embedding encrypted data information identifying the recognized object in the output signal" have been fully considered but they are not persuasive.

Chainer clearly teaches "implementing a recognition algorithm to identifying objects associated with the sensed images" in column 7 lines 52-61 i.e. "the system of the present invention could be easily used to identify animate objects (e.g., people, animals, etc.). In such a case, the animate object can be identified by taking a picture (e.g., obtaining an image) of the animate object while simultaneously obtaining other data (e.g., confirming biometric information such as iris/retinal shape, dental configuration, etc.). Further, the animate objects may carry a tag (e.g., a radio frequency (RF) tag, a magnetic tag, a Smart Card, a bar code, a biometric identifier, etc.). Thus, animate and inanimate objects can be easily authenticated with the present invention."

Chainer also teaches "embedding encrypted data information identifying the recognized object in the output signal" in figure 2 and 3 and column 4 line 30 – 46 i.e. Specifically, the tag ID information from the RF reader 103 is encoded along with a time stamp (e.g., time of output of interrogation pulse and time of receipt of interrogation information from the tag(s)) and other desired information, such as the focal length of

the camera 104, or a hash (e.g., possibly encrypted or non-encrypted) of the digital

image acquired by the camera 104."

Applicant's arguments that Grube does not teach "randomly generating a new

encryption key for encrypting different portions of the video signal over time" have been

fully considered but they are not persuasive. Peters teaches that the video signal is

encrypted in figure 1 and paragraph 0031. Grube teach randomly generating a new

encryption key for encrypting different portions of data over time. In column 1 line 51-67

i.e. "Because of security issues related with secure communication systems, encryption

keys and/or encryption algorithms may be changed within the secure wireless

communication system. To maintain security over a longer period of time, secure

communication systems regularly change the active system encryption parameters,

which include encryption algorithm and encryption key. Such a change may be monthly,

daily, or even hourly depending on the nature of security desired." Because these key

are changed and used they had to have been generated in order to have been used.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains. ·
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 17 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Peters (U.S. 2003/0226023) in view of Kielland et al (U.S. Patent # 6,081,206)

further in view of Grube et al (U.S. Patent # 5,517,568). Peters teaches with respect to

claim 17, a method for generating an output signal from a video data acquisition system,

the method comprising: receiving a video signal that varies depending on sensed

images (see Peters paragraph 0004); encrypting the video signal using a first key (see

Peters figure 1 and paragraph 0031 i.e. then encrypts some part of that captured input

with a symmetric key which has been generated or provided for use with this image file);

encrypting the first key using a second key (see Peters figure 1 and paragraph 0031 i.e.

The symmetric key is then encrypted (Block 120), preferably using public key

encryption); including at least the encrypted first key and encrypted video signal in the

output signal (see Peters paragraph 0032 i.e. Having encrypted both the image and the

symmetric key, the image is then stored on some form of persistent storage). Peters

does not teach implementing a recognition algorithm to identify objects associated with

the sensed images; in response to recognizing an object, embedding encrypted data

information identifying the recognized object in the output signal and randomly

generating a new encryption key for encrypting different portions of the video signal

over time.

Kielland teaches means for identifying objects (see Kielland column 6 line 64 –

column 7 line 11 i.e. License plate) associated with the sensed images (see Kielland

column 6 line 64 – column 7 line 11 i.e. digital camera captures a raster image of each

vehicle) and embedding encrypted data information identifying the recognized object in

the output signal (see Kielland column 6 line 64 – column 7 line 11). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have attached the unique digital identifier for the vehicle to help determine where and when the vehicle was spotted. Therefore one would be motivated to have included object data in the output signal (see Kielland column 6 line 64 – column 7 line 11).

Grube teaches randomly generating a new encryption key for encrypting different portions of the video signal over time (see Grube column 1 line 51-67). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to generating a new encryption key for encrypting different portions of the video signal over time to increase the security of the transfer by changing the encryption thought out the transfer. One would be motivated to have randomly generating a new encryption key for encrypting different portions of the video signal over time to further increase security (see Grube column 1 line 51-67).

With respect to claim 32, an apparatus to support surveillance, the apparatus comprising: a camera to generate a video signal that varies depending on sensed images (see Peters paragraph 0004); a memory device to store at least first and second encryption keys (see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is preferably stored with the encrypted image, but alternatively may be separately stored (e.g., in a separate file)); a processor that

encrypts the video signal using the first encryption key (see Peters figure 1 and

paragraph 0031 i.e. then encrypts some part of that captured input with a symmetric key

which has been generated or provided for use with this image file), the processor

encrypting the first encryption key with the second encryption key (see Peters figure 1

and paragraph 0031 i.e. The symmetric key is then encrypted (Block 120), preferably

using public key encryption), the processor producing an output signal including at least

the encrypted video signal and the encrypted first encryption key (see Peters paragraph

0032 i.e. Having encrypted both the image and the symmetric key, the image is then

stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is

preferably stored with the encrypted image, but alternatively may be separately stored

(e.g., in a separate file)). Peters does not teach a recognition system to identify objects

associated with the sensed images, the processor embedding encrypted data

information identifying the recognized object in the output signal and an encryption key

generator that randomly generates a new value for the first encryption key to uniquely

encrypt different portions of the video signal over time. Kielland teaches means for

identifying objects (see Kielland column 6 line 64 – column 7 line 11 i.e. License plate)

associated with the sensed images (see Kielland column 6 line 64 – column 7 line 11

i.e. digital camera captures a raster image of each vehicle) and embedding encrypted

data information identifying the recognized object in the output signal (see Kielland

column 6 line 64 – column 7 line 11). It would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject

matter pertains to have attached the unique digital identifier for the vehicle to help

determine where and when the vehicle was spotted. Therefore one would be motivated

to have included object data in the output signal (see Kielland column 6 line 64 –

column 7 line 11). Grube teaches an encryption key generator that randomly generates

a new value for the first encryption key to uniquely encrypt different portions of the video

signal over time (see Grube column 1 line 51-67). It would have been obvious at the

time the invention was made to a person having ordinary skill in the art to which said

subject matter pertains to generating a new encryption key for encrypting different

portions of the video signal over time to increase the security of the transfer by changing

the encryption thought out the transfer. One would be motivated to have randomly

generating a new encryption key for encrypting different portions of the video signal

over time to further increase security (see Grube column 1 line 51-67).

Claims 17, 32, 43-47 and 49 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Peters (U.S. 2003/0226023) in view of Chainer et al (U.S. Patent #

6,397,334) further in view of Grube et al (U.S. Patent # 5,517,568).

With respect to claim 17 Peters teaches, a method for generating an output

signal from a video data acquisition system, the method comprising: receiving a video

signal that varies depending on sensed images (see Peters paragraph 0004);

encrypting the video signal using a first key (see Peters figure 1 and paragraph 0031 i.e.

then encrypts some part of that captured input with a symmetric key which has been

generated or provided for use with this image file); encrypting the first key using a

second key (see Peters figure 1 and paragraph 0031 i.e. The symmetric key is then

encrypted (Block 120), preferably using public key encryption); including at least the

encrypted first key and encrypted video signal in the output signal (see Peters

paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image

is then stored on some form of persistent storage);

Peters does not teach implementing a recognition algorithm to identify objects

associated with the sensed images; and in response to recognizing an object,

embedding encrypted data information identifying the recognized object in the output

signal and randomly generating a new encryption key for encrypting different portions of

the video signal over time.

Chainer teaches means for identifying objects associated with the sensed

images and embedding encrypted data information identifying the recognized object in

the output signal (see Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and

column 7 lines 52-61). It would have been obvious at the time the invention was made

to a person having ordinary skill in the art to which said subject matter pertains to have

recognized object based on RFID tags, iris/retinal shape, dental configuration and other

characteristic and transmit then in encrypted from to help the receiver authenticate what

he is looking at. One would be motivated to have sent sensor data encrypted to help the

receiver authenticate what he is looking at (see Chainer column 1 lines 27-51).

Grube teaches randomly generating a new encryption key for encrypting different

portions of the video signal over time (see Grube column 1 line 51-67). It would have

been obvious at the time the invention was made to a person having ordinary skill in the

art to which said subject matter pertains to generating a new encryption key for

encrypting different portions of the video signal over time to increase the security of the

transfer by changing the encryption thought out the transfer. One would be motivated to

have randomly generating a new encryption key for encrypting different portions of the

video signal over time to further increase security (see Grube column 1 line 51-67).

With respect to claim 32, Peters teaches an apparatus to support surveillance,

the apparatus comprising: a camera to generate a video signal that varies depending on

sensed images (see Peters paragraph 0004); a memory device to store at least first and

second encryption keys (see Peters paragraph 0032 i.e. Having encrypted both the

image and the symmetric key, the image is then stored on some form of persistent

storage and 0032 i.e. The encrypted symmetric key is preferably stored with the

encrypted image, but alternatively may be separately stored (e.g., in a separate file)); a

processor that encrypts the video signal using the first encryption key (see Peters figure

1 and paragraph 0031 i.e. then encrypts some part of that captured input with a

symmetric key which has been generated or provided for use with this image file), the

processor encrypting the first encryption key with the second encryption key (see Peters

figure 1 and paragraph 0031 i.e. The symmetric key is then encrypted (Block 120),

preferably using public key encryption), the processor producing an output signal

including at least the encrypted video signal and the encrypted first encryption key (see

Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key,

the image is then stored on some form of persistent storage and 0032 i.e. The

encrypted symmetric key is preferably stored with the encrypted image, but alternatively

may be separately stored (e.g., in a separate file)). Peters does not teach a recognition

system to identify objects associated with the sensed images, the processor embedding

encrypted data information identifying the recognized object in the output signal and an

encryption key generator that randomly generates a new value for the first encryption

key to uniquely encrypt different portions of the video signal over time. Chainer teaches

means for identifying objects associated with the sensed images and embedding

encrypted data information identifying the recognized object in the output signal (see

Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and column 7 lines 52-61).

It would have been obvious at the time the invention was made to a person having

ordinary skill in the art to which said subject matter pertains to have recognized object

based on RFID tags, iris/retinal shape, dental configuration and other characteristic and

transmit then in encrypted from to help the receiver authenticate what he is looking at.

One would be motivated to have sent sensor data encrypted to help the receiver

authenticate what he is looking at (see Chainer column 1 lines 27-51). Grube teaches

an encryption key generator that randomly generates a new value for the first encryption

key to uniquely encrypt different portions of the video signal over time (see Grube

column 1 line 51-67). It would have been obvious at the time the invention was made to

a person having ordinary skill in the art to which said subject matter pertains to

generating a new encryption key for encrypting different portions of the video signal

over time to increase the security of the transfer by changing the encryption thought out

the transfer. One would be motivated to have randomly generating a new encryption

key for encrypting different portions of the video signal over time to further increase security (see Grube column 1 line 51-67).

With respect to claim 43, wherein implementing the recognition algorithm to identify objects associated with the sensed images includes: analyzing one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image (see Chainer column 7 lines 52-61).

With respect to claim 44, wherein embedding encrypted data information identifying the recognized object in the output signal includes: encrypting data identifying objects associated with the sensed images with a third key, the third key being distinct from the first key so that a user, possessing only the third key but not the first key, can decrypt the data identifying objects without having the capability to decrypt the video signal; and including the data encrypted with the third key in the output signal (see Chainer column 4 lines 40-46).

With respect to claim 45, wherein the apparatus further comprises: means for randomly generating a new encryption key for encrypting different portions of the video signal over time (see Chainer column 7 lines 52-61).

With respect to claim 46, wherein the processor, when embedding encrypted data information identifying the recognized object in the output signal: encrypts data identifying objects associated with the sensed images with a third key, the third key being distinct from the first key so that a user, possessing only the third key but not the first key, can decrypt the data identifying objects without having the capability to decrypt

the video signal; and includes the data encrypted with the third key in the output signal

(see Chainer column 4 lines 40-46).

With respect to claim 47, wherein the apparatus further comprises: means for

randomly generating a new encryption key for encrypting different portions of the video

signal over time (see Grube column 1 line 51-67).

With respect to claim 49, wherein the instructions, when carried out by the

processing device, cause the processing device to further perform the step of: randomly

generating a new encryption key for encrypting different portions of the video signal

over time (see Grube column 1 line 51-67).

Claims 37, 38, 48 and 50-52 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Peters (U.S. 2003/0226023) in view of Chainer et al (U.S. Patent #

6,397,334). With respect to claim 37, an apparatus to support surveillance, the

apparatus comprising: a camera to generate a video signal that varies depending on

sensed images (see Peters paragraph 0004); a memory device to store at least first

and second encryption keys (see Peters paragraph 0032 i.e. Having encrypted both the

image and the symmetric key, the image is then stored on some form of persistent

storage and 0032 i.e. The encrypted symmetric key is preferably stored with the

encrypted image, but alternatively may be separately stored (e.g., in a separate file));

means for encrypting the video signal using the first encryption key (see Peters figure 1

and paragraph 0031 i.e. then encrypts some part of that captured input with a

symmetric key which has been generated or provided for use with this image file) and

means for encrypting the first encryption key with the second encryption key (see Peters

figure 1 and paragraph 0031 i.e. The symmetric key is then encrypted (Block 120),

preferably using public key encryption) to produce an output signal including at least the

encrypted video signal and the encrypted first encryption key (see Peters paragraph

0032 i.e. Having encrypted both the image and the symmetric key, the image is then

stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is

preferably stored with the encrypted image, but alternatively may be separately stored

(e.g., in a separate file)). Peters does not teach means for identifying objects associated

with the sensed images and embedding encrypted data information identifying the

recognized object in the output signal wherein embedding encrypted data identifying the

recognized object in the output signal includes: encrypting data identifying objects

associated with the sensed images with a third key, the third key being distinct from the

first key so that a user, possessing only the third key but not the first key, can decrypt

the data identifying objects without having the capability to decrypt the video signal; and

including the data encrypted with the third key in the output signal. Chainer teaches

means for identifying objects associated with the sensed images and embedding

encrypted data information identifying the recognized object in the output signal (see

Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and column 7 lines 52-61)

and wherein embedding encrypted data identifying the recognized object in the output

signal includes: encrypting data identifying objects associated with the sensed images

with a third key, the third key being distinct from the first key so that a user, possessing

only the third key but not the first key, can decrypt the data identifying objects without

having the capability to decrypt the video signal; and including the data encrypted with

the third key in the output signal (see Chainer column 4 lines 40-46). It would have been

obvious at the time the invention was made to a person having ordinary skill in the art to

which said subject matter pertains to have recognized object based on RFID tags,

iris/retinal shape, dental configuration and other characteristic and transmit then in

encrypted from to help the receiver authenticate what he is looking at. One would be

motivated to have sent sensor data encrypted to help the receiver authenticate what he

is looking at (see Chainer column 1 lines 27-51).

With respect to claim 38, a computer program product including a computer-

readable medium having instructions stored thereon for processing data information,

such that the instructions, when carried out by a processing device, cause the

processing device to perform the steps of: receiving a video signal that varies

depending on sensed images (see Peters paragraph 0004); encrypting the video signal

using a first key (see Peters figure 1 and paragraph 0031 i.e. then encrypts some part of

that captured input with a symmetric key which has been generated or provided for use

with this image file); encrypting the first key using a second key, the first and second

key being different than each other (see Peters figure 1 and paragraph 0031 i.e. The

symmetric key is then encrypted (Block 120), preferably using public key encryption);

including at least the encrypted first key and encrypted video signal in the output signal

(see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric

key, the image is then stored on some form of persistent storage and 0032 i.e. The

encrypted symmetric key is preferably stored with the encrypted image, but alternatively

may be separately stored (e.g., in a separate file)). Peters does not teach implementing

a recognition algorithm to identify objects associated with the sensed images, and

embedding encrypted data information identifying the recognized object in the output

signal wherein embedding encrypted data identifying the recognized object in the output

signal includes: encrypting data identifying objects associated with the sensed images

with a third key, the third key being distinct from the first key so that a user, possessing

only the third key but not the first key, can decrypt the data identifying objects without

having the capability to decrypt the video signal; and including the data encrypted with

the third key in the output signal. Chainer teaches means for identifying objects

associated with the sensed images and embedding encrypted data information

identifying the recognized object in the output signal (see Chainer figure 2 and 3,

column 4 line 30 – column 6 line 17 and column 7 lines 52-61) and wherein embedding

encrypted data identifying the recognized object in the output signal includes: encrypting

data identifying objects associated with the sensed images with a third key, the third key

being distinct from the first key so that a user, possessing only the third key but not the

first key, can decrypt the data identifying objects without having the capability to decrypt

the video signal; and including the data encrypted with the third key in the output signal

(see Chainer column 4 lines 40-46). It would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject

matter pertains to have recognized object based on RFID tags, iris/retinal shape, dental

configuration and other characteristic and transmit then in encrypted from to help the

receiver authenticate what he is looking at. One would be motivated to have sent sensor

data encrypted to help the receiver authenticate what he is looking at (see Chainer column 1 lines 27-51).

With respect to claim 48, wherein the means for identifying objects associated with the sensed images includes means for analyzing one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image (see Chainer column 7 lines 52-61).

With respect to claim 50, wherein the step of identifying objects associated with the sensed images includes analyzing one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image (see Chainer column 7 lines 52-61).

With respect to claim 51, a method for generating an output signal from a video data acquisition system, the method comprising: receiving a video signal that varies depending on sensed images (see Peters paragraph 0004); encrypting the video signal using a first key (see Peters figure 1 and paragraph 0031 i.e. then encrypts some part of that captured input with a symmetric key which has been generated or provided for use with this image file); encrypting the first key using a second key (see Peters figure 1 and paragraph 0031 i.e. The symmetric key is then encrypted (Block 120), preferably using public key encryption); including at least the encrypted first key and encrypted video signal in the output signal (see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is preferably stored with the encrypted image, but alternatively may be separately stored (e.g., in a separate file)).

Peters does not teach implementing a recognition algorithm to identify objects

associated with the sensed images; and in response to recognizing an object,

embedding encrypted data identifying the recognized object in the output signal;

wherein embedding encrypted data identifying the recognized object in the output signal

includes: encrypting data identifying objects associated with the sensed images with a

third key, the third key being distinct from the first key so that a user, possessing only

the third key but not the first key, can decrypt the data identifying objects without having

the capability to decrypt the video signal; and including the data encrypted with the third

key in the output signal. Chainer teaches means for identifying objects associated with

the sensed images and embedding encrypted data information identifying the

recognized object in the output signal (see Chainer figure 2 and 3, column 4 line 30 –

column 6 line 17 and column 7 lines 52-61) and wherein embedding encrypted data

identifying the recognized object in the output signal includes: encrypting data

identifying objects associated with the sensed images with a third key, the third key

being distinct from the first key so that a user, possessing only the third key but not the

first key, can decrypt the data identifying objects without having the capability to decrypt

the video signal; and including the data encrypted with the third key in the output signal

(see Chainer column 4 lines 40-46). It would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject

matter pertains to have recognized object based on RFID tags, iris/retinal shape, dental

configuration and other characteristic and transmit then in encrypted from to help the

receiver authenticate what he is looking at. One would be motivated to have sent sensor

data encrypted to help the receiver authenticate what he is looking at (see Chainer

column 1 lines 27-51).

With respect to claim 52, wherein implementing the recognition algorithm to

identify objects associated with the sensed images includes: analyzing one sensed

image of the sensed images to identify a person associated with a pattern depicted in

the one sensed image (see Chainer column 7 lines 52-61).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Devin Almeida whose telephone number is 571-270-

1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to
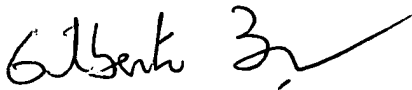
5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to

4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Devin Almeida
Patent Examiner
1/10/2008

GILBERTO BARRON Jr
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100